WHAT IS CLAIMED IS:

1.   A method of mirroring security processors comprising the steps of:

generating information for a first security processor;

repeatedly sending the information to a second security processor in accordance with the first security processor processing at least one packet.

2.   The method of claim 1 wherein the sending step comprises sending the information from the first security processor to the second processor.

3.   The method of claim 1 wherein the generating step comprises generating the information in the first security processor.

4.   The method of claim 1 further comprising the step of generating at least one packet including the information, wherein the sending step comprises sending the at least one packet over a packet network.

5.   The method of claim 1 wherein the sending step further comprises sending the information over a dedicated link between the first security processor and the second security processor.

6.   The method of claim 5 wherein the dedicated link comprises an Ethernet link.

7.   The method of claim 1 wherein the sending step comprises repeatedly sending the information on a per-packet basis.

8.   The method of claim 1 wherein the sending step comprises repeatedly sending the information at intervals according to at least one sequence number.

9.   A method of mirroring security processors comprising the steps of:

generating security association information for a first security processor; and

repeatedly sending the security association information to a second security processor in accordance with the first security processor processing at least one packet.

10.   The method of claim 9 wherein the information comprises at least one security association sequence number.

11.   The method of claim 9 wherein the information comprises at least one security association byte count.

12.   The method of claim 9 wherein the sending step further comprises repeatedly sending the security association information on a per-packet basis.

13.   The method of claim 9 wherein the sending step further comprises repeatedly sending the security association information at intervals according to at least one sequence number.

14.   The method of claim 9 further comprising the step of generating at least one packet including the security association information, wherein the sending step comprises sending the at least one packet.

15.   The method of claim 9 further comprising the step of generating at least one packet including the security

18

association information, wherein the sending step comprises sending the at least one packet over a packet network.

16. The method of claim 9 wherein the sending step further comprises sending the information over a dedicated link between the first security processor and the second security processor.

17. The method of claim 16 wherein the dedicated link comprises an Ethernet link.

18. A method of providing redundancy in a security processing system comprising the steps of:

establishing secure packet flow through a first security processor;

modifying security association information associated with the secure packet flow;

sending the modified security association information to a second security processor; and

rerouting the secure packet flow to flow through the second security processor instead of the first security processor.

19. The method of claim 18 wherein the rerouting step is in response to a failure of packet flow through the first security processor.

20. A method of mirroring security association information comprising the steps of:

receiving, by a first security processor, at least one packet;

modifying security association information associated with the at least one packet;

19

storing the modified security association information in a first data memory;

sending the modified security association information to a second security processor; and

5   storing, by the second security processor, the modified security association information in a second data memory.

21. The method of claim 20 wherein the security association information comprises at least one sequence number.

10   22. The method of claim 20 wherein the security association information comprises at least one byte count.

23. The method of claim 20 wherein the sending step further comprises repeatedly sending the security association information.

15   24. The method of claim 20 wherein the sending step further comprises repeatedly sending the security association information at intervals according to at least one sequence number.

25. The method of claim 20 further comprising the step
20 of generating at least one configuration packet including the security association information, wherein the sending step comprises send the at least one configuration packet.

26. The method of claim 20 further comprising the step of sending, by a host processor, configuration information to
25 the first security processor and the second security processor.

27. The method of claim 20 further comprising the step of sending, by a host processor, security association configuration information to the first security processor and the second security processor.

5   28. The method of claim 20 further comprising the step of updating security association information for at least one outbound packet.

29. The method of claim 28 further comprising the steps of:

10   defining a quantity to adjust a sequence number;

defining an interval at which to update the security association information; and

determining whether to send the security association information to the second security processor according to a

15   comparison of a sequence number with the interval.

30. The method of claim 29 further comprising adding the quantity to the sequence number before sending the security association information to the second security processor.

31. The method of claim 20 further comprising the step

20   of updating security association information for at least one inbound packet.

32. The method of claim 31 further comprising the steps of:

defining a quantity to adjust a sequence number;

25   defining a width of a replay window; and

determining whether to send the security association information to the second security processor according to a comparison of a sequence number with the width.

21

33.   The method of claim 32 further comprising the step of adding the quantity to the sequence number before sending the security association information to the second security processor.

5   34.   The method of claim 32 further comprising the step of sending replay window information to the second security processor.

35.   A security processing system, comprising:

a first security processor for processing packets and for
10 updating security association information associated with the packets, the first security processor comprising at least one MAC for sending updated security association information over a packet network; and

a second security processor for receiving the updated
15 security association information over the packet network.

36.   The security processing system of claim 35 further comprising at least one host processor connected to the first security processor and the second security processor for terminating or initiating the packets.

20   37.   The security processing system of claim 36 wherein the at least one host processor changes the routing of packet flow by either routing the packets to the second security processor instead of the first security processor.

38.   A security processing system, comprising:
25   a first security processor for processing a first packet flow, updating security association information in response to the first packet flow and sending the updated security association information to a second security processor;

22

a second security processor for processing a second packet flow, updating security association information in response to the second packet flow and sending the updated security association information to the first security

5   processor; and

at least one switch for routing the first packet flow and the second packet flow to the first security processor and the second security processor.

39.   The security processing system of claim 38 further

10   comprising at least one host processor connected to the at least one switch for terminating or initiating the first packet flow and the second packet flow.

40.   The security processing system of claim 39 wherein the at least one host processor changes the routing of packet

15   flow by either routing the first packet flow to the second security processor instead of the first security processor or routing the second packet flow to the first security processor instead of the second security processor.

41.   The security processing system of claim 40 wherein

20   the change in the routing is in response to a failure of the first packet flow through the first security processor or the second packet flow through the second security processor.

42.   A security processing system, comprising:

at least one host processor for establishing a first

25   packet flow to a first security processor and a second packet flow to a second security processor;

a first security processor for updating a first set of security association information associated with the first packet flow and sending the updated first set of security

30   association information to a second security processor; and

a second security processor for updating a second set of security association information associated with the second packet flow and sending the updated second set of security association information to the first security processor.

5   43.   The security processing system of claim 42 wherein the at least one host processor routes the first packet flow to the second security processor instead of the first security processor.

       44.   The security processing system of claim 42 wherein
10   the at least one host processor routes the second packet flow to the first security processor instead of the second security processor.